Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF INTERFED SECURITY AND CONTROLS

OFFICE OF INSPECTOR GENERAL

(A9711) **March 1998**

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

March 31, 1998

Mr. Stephen R. Malphrus, Director
Division of Information Resources Management

This letter report represents the results of our *Audit of InterFed Security and Controls* (A9711). We performed this audit in conjunction with a Systemwide audit of InterFed led by the Federal Reserve Bank of Richmond.[1]

As you know, InterFed is a private Internet Protocol (IP) router network linking all twelve Federal Reserve Districts, the Federal Reserve Automation Services (FRAS) and the Board of Governors of the Federal Reserve System (the Board). The components of the InterFed gateway consist of a local (District or Board) router, a national router, and the InterFed LAN Segment (ILS) connecting the two routers (See appendixes 1 and 2 for a high-level diagram of the architecture). Because the InterFed connects to external, non-Federal Reserve networks (e.g. via the Internet), the System is subject to the risk that unauthorized users could gain access to the Board's networks and mainframe. Recent research shows that this risk is increasing; the Computer Security Institute's Annual Computer Security Survey respondents reported a 10% increase in 1997 in attacks on their systems via the Internet. The survey also noted that 249 organizations out of 563 responses reported financial losses from attacks by unauthorized users totaled $100 million.

The overall objective for the InterFed Security and Controls audit was to evaluate the adequacy and effectiveness of the system of internal controls as established by FRAS, Reserve Bank, and Board management over the InterFed IP router network and Internet access gateways. The audit also covered the following related areas: (1) policies and procedures concerning external service(s) connections (outbound telecommunications only); (2) dial-in access; (3) configuration of the Board's InterFed router as well as logical access controls and physical security of the router; (4) the Board's anti-virus policies and procedures, including user training and awareness programs; (5) Century Date Change (CDC) compliance status of the Board's InterFed router and associate hardware/software; and
(6) contingency planning. To accomplish our objective, we interviewed Board staff, reviewed Board policies, procedures and related documentation, performed selective testing in several of

[1] In addition to the local and national InterFed reviews, audits of the System's Firewalls at the Board and the Federal Reserve Banks of Boston and New York are also being performed. The Firewall audit will be reported separately.

the Board's divisions and offices, and relied on recent audit findings from audits of the Divisions of Reserve Bank Operations and Payment Systems, Consumer & Community Affairs, and Banking Supervision & Regulation. We also participated in Systemwide conference calls with District audit representatives to review potential audit findings and ensure consistent treatment.

In general, we found that the Board has implemented appropriate controls and safeguards to protect the InterFed network from unauthorized access and disruption and therefore have no formal recommendations. However, we identified opportunities for improvement in the related areas of anti-virus policies and procedures, external services, risk certification, and dial-in access; the technical findings for these items will be provided to you in a separate letter.

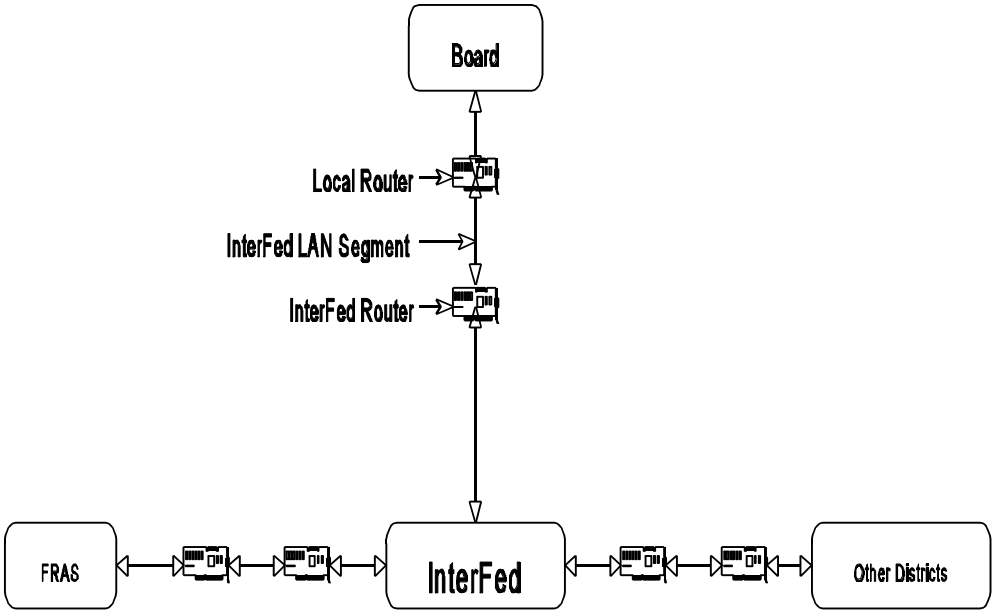
Copies of this report are being provided to the Administrative Governor, the Staff Director for Management, and the General Auditor of the Federal Reserve Bank of Richmond who has System reporting responsibility for this audit. The report is available to the public and a summary will appear in our next semiannual report to the Congress. We are also making the report available on our Internet web page which is located at *http://www.ignet.gov/ ignet/internal/frb/oighome.html*. We appreciate the cooperation, courtesy and assistance provided by your staff to us during the performance of this audit. If you have questions regarding this audit or other issues, please feel free to call me at extension 5003.

Sincerely,

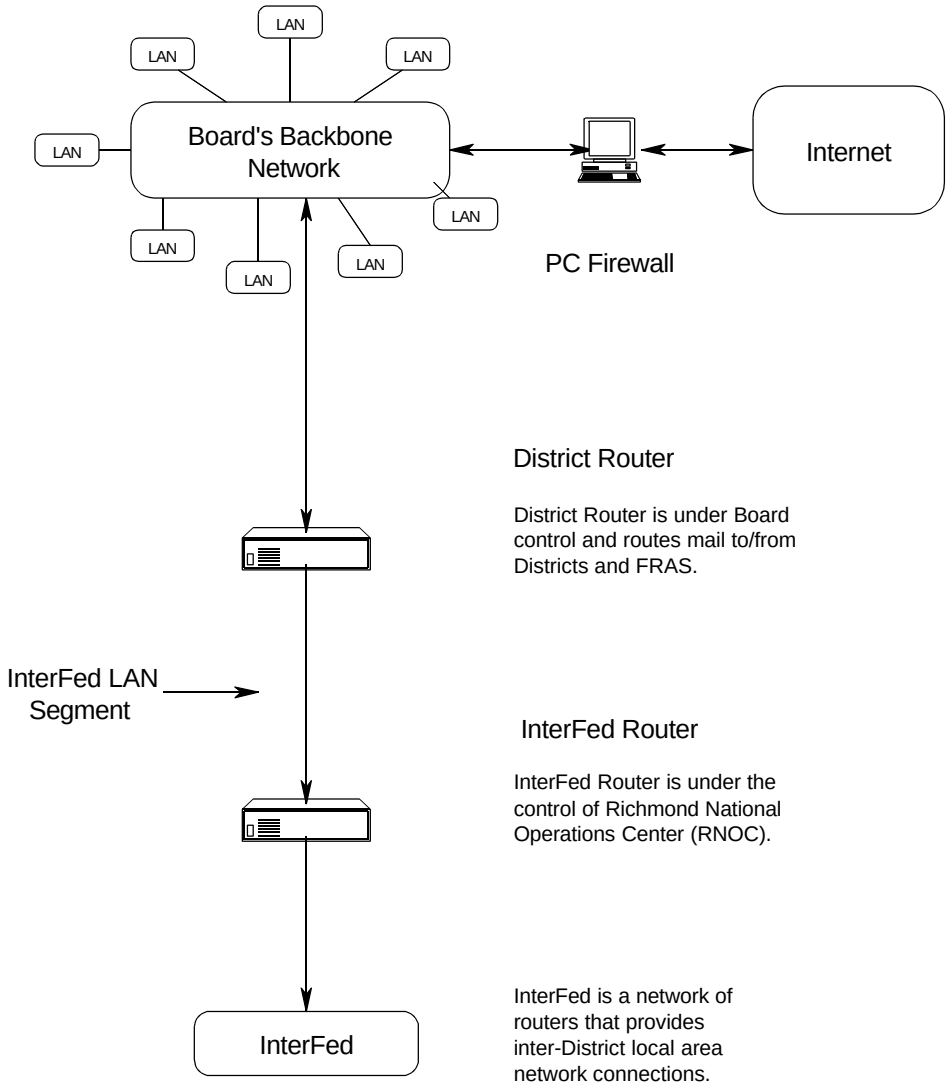
Barry R. Snyder
Assistant Inspector General for Audit

APPENDIXES

Appendix 1 - System's InterFed Architecture



Appendix 2 - Board's InterFed Architecture



Appendix 3 - Principal OIG Contributors to this Report

Emily Drake, EDP-Auditor and Auditor-in-Charge

Dave McCue, Auditor

Patty Kelley, Audit Manager

Barry Snyder, Assistant Inspector General for Audits